UNITED STATES PATENT AND TRADEMARK OFFICE

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/468,157	12/21/1999	JAMES H. MOORE	D/99748	3291

7590 10/29/2003	EXAMINER
JOHN E BECK	SHIN, KYUNG H
XEROX CORPORATION	

	ART UNIT	PAPER NUMBER
XEROX SQUARE 20A	2132	
ROCHESTER, NY 14644		

DATE MAILED: 10/29/2003

Please find below and/or attached an Office communication concerning this application or proceeding.

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE <u>3</u> MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
- Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on <u>*21 December 1999*</u> .

2a) ☐ This action is **FINAL.**   2b) ☒ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) <u>*1-5*</u> is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) <u>*1-5*</u> is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

11) ☐ The proposed drawing correction filed on _____ is: a)☐ approved b)☐ disapproved by the Examiner.

   If approved, corrected drawings are required in reply to this Office action.

12) ☐ The oath or declaration is objected to by the Examiner.

Priority under 35 U.S.C. §§ 119 and 120

13) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a)☐ All b)☐ Some * c)☐ None of:

   1.☐ Certified copies of the priority documents have been received.

   2.☐ Certified copies of the priority documents have been received in Application No. _____ .

   3.☐ Copies of the certified copies of the priority documents have been received in this National Stage
   application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

14) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. § 119(e) (to a provisional application).

   a) ☐ The translation of the foreign language provisional application has been received.

15) ☐ Acknowledgment is made of a claim for domestic priority under 35 U.S.C. §§ 120 and/or 121.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)   4) ☐ Interview Summary (PTO-413) Paper No(s). _____ .
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)   5) ☐ Notice of Informal Patent Application (PTO-152)
3) ☐ Information Disclosure Statement(s) (PTO-1449) Paper No(s) _____ .   6) ☐ Other: .

DETAILED ACTION

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

The factual inquiries set forth in *Graham* v. *John Deere Co.*, 383 U.S. 1, 148 USPQ 459

(1966), that are applied for establishing a background for determining obviousness

under 35 U.S.C. 103(a) are summarized as follows:

1.   Determining the scope and contents of the prior art.
2.   Ascertaining the differences between the prior art and the claims at issue.
3.   Resolving the level of ordinary skill in the pertinent art.
4.   Considering objective evidence present in the application indicating obviousness or nonobviousness.

Claim 1- 4 are rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al.

U.S. Patent No. 5,136,647 in view of Romney et al. U.S. Patent No. 6,085,322 and

further in view of Doyle U.S. Patent No. 6,381,696.

In regard to independent **claim 1,** Haber discloses a method of time stamping digital

document (see Fig1 and col. 2, line33) and verify by signatures (see col. 2, line 44) to

accept integrity of document on a reliable system prior to its transmittal to the author.

Haber discloses:

a) The client (author) converts the digital document to a reduced digital size (see

   col. 3, line 9-11) using one-way hash (see col. 3, line 13) to meet the step of

   transmitting encrypted data;

b) TSP (Time Source Provider) creating a TimeMap as Time stamp receipt (see

   Fig. 2, step 25) containing a current time (see col. 4, line 10-12), an ID of

   author, a hash of document, and receipt of the data, etc for each document

   (see col. 4, line 8) with a variety of parameters as a string (see col. 6, line 24),

   and cryptographic signatures (see col. 6, line 28-30);

c) TSP returns client's data along with the certified (e.g., signature) TimeMap

   (see col. 4, line 23) and encryption key signatures (see col. 7, line 2);

d) TSP providing encrypted data (see step 27 and col. 6, line 57) back to the

   client (author) (see col. 6, line 68);

However, Haber does not disclose the client generating a key pair; generating

"attributes" including "cryptographic signatures"; encrypting the file with client's public

key. Haber does not disclose the client archives the original files, file attributes and time

map from TSA. However, Romney discloses:

a) the client generating a Public and a Private Key pair (see Fig. 2, 200 and col.

   6, line 62, 63);

b) the client generate cryptographic signature (col. 7, line 51, 52) and attached

   to the document (col. 7, line 60);

c) encrypting the client's files, message digest, with the private key (see col. 8,

   line 42);

Doyle discloses:

a) returning the client data (see col. 7, line 38) along with the session key

signatures (see col. 8, line 56).

It would have been obvious to one of the ordinary skilled in the art at the time

the invention was made to modify Haber to generate a Public and a Private

key pair (see col. 6, line 62, 63) and signature the encrypted data as taught in

Romney. Further in view to modify Haber by providing signature for the time

stamped file attest to the veracity of both the content of the original data, as

well as the timestamp at which the session key signature was made as taught

in Doyle.

One would have been motivated to modify Haber to create a key pair and

signature by client as taught in Romney in order to prevent altering the

document during transmission (see col. 2, line 62, 63) from the sender to the

recipient. Further, one would have been motivated to modify Haber to sign

the TimeMap with the session key signature based on time differences as

taught in Doyle in order to authenticate digital signature time stamps with a

pair of signature keys, because signing time stamped file with a session key

signature prevents tampering, which provides non-repudiation to the client

authenticity (see col. 4, line 10).

In regard to **claim 2** Romney discloses the client's Public/Private Key pair (see Fig. 3A,

step 2010 and col. 5, line 34) is organizationally associated.

In regard to **claim 3** Doyle discloses the client provides multiple encryption of files, generating the signature of the file at each step, and providing all signatures along with the encryption key signatures (see col. 8, line 56 and 65)

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Haber's time-stamp signature process to incorporate a multiple encryption of files in generating the signatures (see col. 9, line 24-28) of the encrypted files with the prepared key pairs as taught in Doyle. One would have been motivated to generate encrypt signature keys for preserving the security in order to provide rigorous proof of the time of existence and the authenticity of the content of documentation (see col. 8, line 56-58).

In regard to **claim 4** Haber discloses including a sequential receipt number in generating the signatures of the encrypted files (see col. 4, line 9). However, Haber does not teach a session key in generating the signature of the encrypted files between the client and Time Source Provider for securing the transaction. However, Doyle teaches a session key (see col. 9, line 19, 20) usage in generating the signatures of the encryption of files and for securing the transaction.

It would have been obvious to one of ordinary skill in the art at the time of the invention to modify Haber's time-stamp signature procedure to incorporate a secret key as the session key (see col. 2, line 39) in generating the signature of the encrypted files as taught in Doyle. One would have been motivated to generate a random session key and encrypt it using a public key in order to

secure document traffic and destroyed when it is no longer needed which reduces the risk of compromising the key.

In regard to **claim 5** is rejected under 35 U.S.C. 103(a) as being unpatentable over Haber et al. U.S. Patent No. 5,136,647 in view of Doyle U.S. Patent No. 6,381,696 and further in view of Labozzeta U.S. Patent No. 5,107,269.

Haber discloses sequential numbers as a modification of the file attributes. Doyle discloses for application of the representation of the time and session key signatures (see col. 8, line 56). But, neither of them teach the application of multiple nor differing error-correcting codes. However, Labozzeta discloses multiple or differing error correcting codes (see col. 4, line 8) with source calibration data (see col. 5, line 48) to generate variable value.

It would have been obvious to one of ordinary skill in the art at the time the invention to modify Haber's time-stamp signature procedure to add the key transmitting with some kind of error detection and correction bits by adapting the error correction (see col. 4, line 18) codes taught in Labozzeta. One would have been motivated to apply representation of time and error correction codes for correcting differential in the detected value in order to prevent a garbled key in transmission to produce a precise measure of the key values and the integrity of documentation with an electronic time stamp.

Conclusion

The prior art made of record and not relied upon is considered pertinent to applicant's disclosure.

- U.S. Patent No. 6,393,126 to van der Kaay et al. discloses System and Methods for Generating Trusted and Authenticble Time Stamps for Elctronic Documentatis

- U.S. Patent No. 5,189,700 to Blandford, Robert R. discloses Device to supply Authenticated Time and Time Stamp and Authenticate Digital Documents

- U.S. Patent No. 6,367,013 to Bisbee et al. discloses System and Methods for Elctronic Transmission, Storage and Retrival of Authenticated Elctronic Original Documents

Any inquiry concerning this communication or earlier communications from the examiner should be directed to Kyung H Shin whose telephone number is 703-305 - 0711. The examiner can normally be reached on 6:30 am - 4:30 pm.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Gilberto Barron can be reached on 703-305-1830. The fax phone numbers for the organization where this application or proceeding is assigned are 703-746-5447 for regular communications and 703-746-8360 for After Final communications.

Any inquiry of a general nature or relating to the status of this application or proceeding should be directed to the receptionist whose telephone number is 703-305-2394.

Kyung H Shin
Examiner
Art Unit 2132

GILBERTO BARRON
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100

Art Unit: 2132

KHS
October 8, 2003